

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANTS

I, Craig A. Graham, being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this Affidavit in support of an application for a search warrant for information associated with a certain TikTok account that is stored at premises owned, maintained, controlled, or operated by TikTok Inc. (“TikTok”), a company headquartered at 5800 Bristol Parkway, Suite 100, Culver City, California. The information to be searched is described in the following paragraphs and in Attachment A-1. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require TikTok to disclose to the government records and other information (including the content of communications) further described in Section I of Attachment B-1. Upon receipt of the information described in Section I of Attachment B-1, government-authorized persons will review that information to locate items described in Section II of Attachment B-1.

2. I also make this Affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. (“Meta”), a company headquartered at 1 Meta Way, Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A-2. This Affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Meta to disclose to the government copies of the information (including the content of communications)

further described in Section I of Attachment B-2. Upon receipt of the information described in Section I of Attachment B-2, government-authorized persons will review that information to locate the items described in Section II of Attachment B-2.

3. I am a Special Agent with Federal Bureau of Investigation (“FBI”), and I am assigned to the Providence office of FBI’s Boston Field Office. I have been an FBI agent since 2010. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including, but not limited to, violations of 18 U.S.C. §§ 2422 and 2252. I have received training in the investigation of internet crimes, child exploitation, transportation of minors, and child sexual abuse, and I have observed and reviewed examples of child pornography, as defined in 18 U.S.C. § 2256. Moreover, I am a federal law enforcement officer authorized by law to request a search warrant.

4. The statements in this Affidavit are based on information provided by law enforcement officers employed by the Rhode Island West Warwick Police Department as well as on my investigation. This Affidavit does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to assess the existence of probable cause for the requested warrants.

5. As described below, there is probable cause to believe that violations of 18 U.S.C. § 2422(b) (persuade, induce, entice, or coerce an individual less than eighteen years of age to engage in sexual activity for which any person can be charged with a criminal offense) and 18 U.S.C. §2252(a)(2) (receipt of child pornography) (collectively, the “SUBJECT OFFENSES”) have been committed by the user of these accounts. There is also probable cause to search the

information described in Attachments A-1 and A-2 for evidence, contraband, and/or fruits of these crimes, as further described in Attachments B-1 and B-2.

PROBABLE CAUSE

6. On March 8, 2024, a resident of West Warwick reported to the West Warwick Police Department (hereinafter “WWPD”) that her minor daughter had been sexually assaulted by an adult male on or around December 30, 2023. The minor was identified as a 14-year-old female born in 2009 (hereinafter “MINOR 1”).

7. Law enforcement officers spoke with MINOR 1’s mother, and MINOR 1 was interviewed by both a physician at the Aubin Center in Providence, and a Forensic Interviewer at the FBI Providence office. Officers learned from MINOR 1 that in or around December of 2023, she communicated with an individual through the mobile application TikTok¹ and sent the individual multiple images of herself nude (in full or in part) and one video of herself nude (in full or in part) at the individual’s request. MINOR 1 later identified the individual’s TikTok account as having a display name of “tacobell999\$\$\$” and a username of “@tacobell99948.” MINOR 1 advised that she communicated with the same individual on Instagram² and identified the individual’s Instagram account as either “kwakle” or “kwaxle.”

¹ TikTok is a social media application developed and owned by Chinese Internet company ByteDance. TikTok is a short-form video hosting service which allows users to view and post short videos. Users can also comment on videos and directly message other users. The application uses the device’s data plan or Wi-Fi to transmit and receive content.

² Instagram is a social media application developed and owned by Meta Platforms, Inc. Instagram allows users to view and post images. Users can also comment and directly message other users. The application uses the device’s data plan or Wi-Fi to transmit and receive content.

8. MINOR 1 provided her own account information for the accounts that she used to communicate with the individual to law enforcement during her forensic interview. She provided her TikTok account as “juvajanga” and her Instagram account as “2fine4youbbyyy.”

9. Preservation letters for all of these accounts were sent to the respective social media companies.

10. MINOR 1 also disclosed to the interviewers that on or about December 30, 2023, she snuck out of her mother’s house to meet the same individual in person. The individual also communicated that he wanted to pay MINOR 1 \$200 to let him perform oral sex on her.

11. I know through my training and experience that TikTok and Instagram are social media applications that are commonly accessed using a cell phone. MINOR 1 stated that the individual who communicated with her through those social media applications, also communicated with her while he was traveling to meet her.

12. MINOR 1 described the individual she met as having long brown hair, a brown beard, and wearing glasses. In her conversations with the individual in person and online, he stated that he was from Newport, RI, was 29 years old, and was named “Pat.” MINOR 1 stated that she may have initially told Pat that she was 16, but that she later communicated and he understood that she was 14 years old.

13. MINOR 1 described the vehicle Pat arrived in as a white van which had the rear seats removed. MINOR 1 first sat in the front passenger seat of the van while talking to Pat. They then moved to the back of the van, where Pat pulled up MINOR 1’s sweatshirt and kissed her chest. Pat then pulled her sweatpants and underwear down, and his lips and tongue touched

her vagina. Pat's penis and fingers also touched the inside of MINOR 1's vagina. At the end of the encounter, Pat gave MINOR 1 two hundred dollars.

14. WWPD obtained consent to search MINOR 1's cell phone. An extraction of the phone's contents was performed and the results of the extraction was reviewed by FBI Providence. The telephone number associated with MINOR 1's device was found to be 401-545-6807. MINOR 1's mother advised law enforcement that she had been in control of MINOR 1's phone since approximately February 9, 2024. Prior to that time, MINOR 1 had blocked @tacobell99948's account. MINOR 1's mother unblocked @tacobell99948 and communicated with the account through MINOR 1's TikTok account. MINOR 1's mother said that she engaged in the communications to learn more about the user of @tacobell99948.

15. A review of the cellphone extraction for images identified multiple images of what appear to be MINOR 1 disrobed. The images depict what appears to be MINOR 1's nude torso, including her breasts and vulva. The images appear to be taken by MINOR 1 using a mirror. This review did not include a review of image transmission information.

16. A review of the cellphone extraction identified communications from February 21, 2024 to March 10, 2024 between MINOR 1's TikTok account (which at the time was being used by MINOR 1's mother) and TikTok account @tacobell99948. In the following communications @tacobell99948 communicated that he wanted to have sexual relations with MINOR 1:

02/22/2024 - 3:35pm	MINOR 1's account	still tryna link?
02/22/2024 - 3:36pm	@tacobell99948	Ya hbu Thinkin bout u m
02/22/2024 - 3:39pm	MINOR 1's account	Wat you thinkin about

02/22/2024 - 3:39pm	@tacobell99948	Smashin u
02/22/2024 - 3:41pm	MINOR 1's account	tell me more
02/22/2024 - 3:42pm	@tacobell99948	Ur right lll bod Wanna eat u out
02/22/2024 - 3:39pm	MINOR 1's account	Wat you thinkin about
02/22/2024 - 3:39pm	@tacobell99948	Smashin u
02/22/2024 - 3:41pm	MINOR 1's account	tell me more
02/22/2024 - 3:42pm	@tacobell99948	Ur right lll bod Wanna eat u out Taste u Wanna smash u so bad m U like? lol u rly busy rn it ok
03/08/2024 - 3:42pm	@tacobell99948	[a link was sent which was no longer accessable]
03/10/2024 - 6:20pm	@tacobell99948	Wanna link wid u

17. Consent was also obtained to search MINOR 1's iPad. An extraction of the iPad's contents was performed and images obtained through the extraction were reviewed by FBI Providence. That review found a video that depicts a female inserting a toothbrush handle into her vagina. The video shows only the female's vagina and hand. That review did not include a review of video transmission information.

18. A subpoena was issued to TikTok for account information related to the account @tacobell99948. TikTok provided the following subscriber information:

Username: tacobell99948

Signup Device Info: iPhone15,4

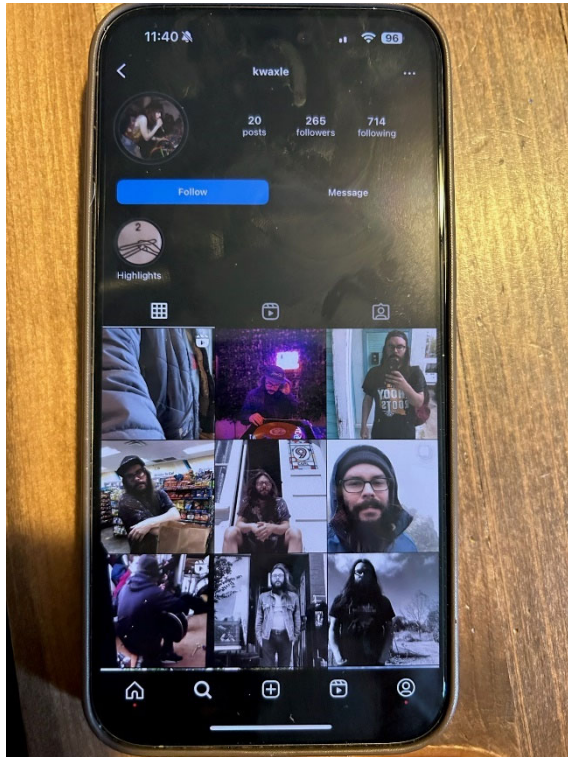
Signup date 01/03/2024 05:25:13am (UTC)

Phone number: +14013740760

Email: drewdrewdrew134@yahoo.com

19. MINOR 1's mother also provided law enforcement with a screen shot of the Instagram account "kwaxle." MINOR 1's mother obtain the screen shot by navigating to the Instagram account using her own cellular telephone. MINOR 1's mother found the kwaxle account based on MINOR 1's recollection of the account's name and MINOR 1 later identified the adult male depicted in the screen shot as Pat, the individual she had sexual relations with on or about December 30, 2023.

20. WWPD was able to identify the individual depicted in the kwaxle account as Kyle Patrick TORMEY, born in 1984. A search of law enforcement databases indicated that TORMEY's home address was 19 Caleb Earl Street, Newport, Rhode Island. A comparison of TORMEY's driver's license photo indicated that TORMEY was the individual depicted on the kwaxle account. The kwaxle account also displayed an image of TORMEY sitting in front of a door that was identified as the front door to 19 Caleb Earl Street, Newport, Rhode Island. Below are images of the kwaxle account and TORMEY's driver's license photo:



21. A subpoena was issued to Instagram for account information related to the account kwaxle. Subscriber information for the account indicated a verified email address of kwaxledelic@gmail.com. A subpoena was then issued to Google for account information related to kwaxledelic@gmail.com and the following subscriber information was returned:

Name: kyle bobyle

Recovery email: kylesantiques@gmail.com

22. A subpoena issued to Google for account information related to kylesantiques@gmail.com returned the following subscriber information:

Name: kyle tormey

Recovery email: vinylgururecordshop@gmail.com

Recovery SMS: +4013740760

23. Open-source searches indicated that TORMEY is an owner/operator of Vinyl Guru Record Shop located at 154 Broadway, Newport, RI 02840 and that telephone 401-374-0760 is associated with Vinyl Guru Record Shop on multiple websites. Surveillance also observed TORMEY entering and exiting Vinyl Guru Record Shop located at 154 Broadway, Newport, Rhode Island, and observed posted business hours of the shop as 12pm to 6pm. The telephone number associated with Vinyl Guru Record Shop is the same number included in the subscriber information for TikTok account @tacobell99948 and the same telephone number in the subscriber information for the recovery email address of the email used to create Instagram account kwaxle. The TikTok communications which occurred between MINOR 1's account and @tacobell99948 occurred during the posted business hours of the Vinyl Guru Record Shop.

24. A subpoena issued to Verizon for account information related to telephone number 401-374-0760 returned information indicating that account was associated with Mary Tormey of Swansea, Massachusetts. A law enforcement database indicated that Kyle TORMEY's mother's name is Mary Tabor. A search of Department of Motor Vehicle records indicated that Mary Tabor has an alias of Mary Tormey and lives at the same Swansea, MA, address as that associated with telephone number 401-374-0760.

25. Department of Motor Vehicles records also indicated that a white 2011 Ford, Massachusetts registration 1HLB49, is registered to Mary Tabor at the same Swansea, MA, address. Law enforcement records described the 2011 Ford as a transit van. Subpoenaed records from the Rhode Island Turnpike and Bridge Authority indicated that 1HLB49 traveled

Westbound over the Newport Bridge at approximately 6:55pm on December 30, 2023, and returned Eastbound over the Newport Bridge at approximately 12:11am on December 31, 2023.

26. Surveillance conducted on March 14, 2024, observed TORMEY sitting in the open doorway of 19 Caleb Earl Street smoking a cigarette. Additionally, a subpoena issued to Rhode Island Energy returned customer information indicating that TORMEY has an active electric and gas account for 19 Caleb Earl Street with a provided customer telephone number of 401-374-0760.

27. All of the above facts and circumstances taken together lead your Affiant to believe that evidence of the offenses under investigation is located, stored or contained at the property, premises, or place identified and described in Attachments A-1 and A-2 of this application for search warrant.

BACKGROUND CONCERNING TIKTOK³

28. TikTok Inc. owns and operates TikTok, a free video social media application for making and sharing short videos. TikTok hosts a variety of short-form user videos ranging in durations from 15 seconds to three minutes.

29. TikTok offers users the ability to create an identity within the application referred to as a “username.” The username is unique to the account and is displayed in their TikTok profile. TikTok obtains and stores subscriber information, video content, user interactions, log data, among other information.

³ The information in this section is based on information published by TikTok Inc. on its TikTok website, including, but not limited to, the following webpage: <https://www.tiktok.com/legal/law-enforcement?lang=en>.

30. TikTok maintains subscriber information including data about its users. I know based on my training and experience that social network providers like TikTok typically ask each of their subscribers to provide certain personal identifying information when registering for an account. This information can include the subscriber's name, physical address, and other identifiers. I know based on my research of TikTok that it records and stores subscriber information, which often includes the username, email address, phone number, device model of the device that users access their account with, account creation date, and Internet Protocol ("IP") address.

31. TikTok stores video content including videos and other multimedia created and modified by TikTok users. I know based on my training and experience that even if this content is removed, locked, or deleted, often social media companies retain the data on their information systems. I know based on my research of TikTok, that it appears to store data that has been made private, locked, or deleted by its users.

32. TikTok maintains records of user interactions, or how TikTok users communicate with each other. I know based on my training and experience that social media platforms like TikTok often include internal messenger systems in which users can interact, send each other direct messages, and react to each other's content in different ways. Based on my research of TikTok, I know that the application allows each other to interact each other through commenting on videos, direct messages, and live chats. TikTok stores this data.

33. TikTok maintains log data regarding its users' use of the app. I know from my training and experience that social media platforms often create detailed analytics of when their users log in to the application, the dates and times of their content creation or internal messages,

and other “metadata.” I know from my research of TikTok that the application collects metadata of its users including login/logout records, dates and times of media creation and modification, dates and time in in-app communications, and other data.

34. Additionally, based on my training and experience, I know that social network providers like TikTok typically maintain records of their users’ communications with the provider. This often includes communications regarding issues relating to their account, such as technical problems or complaints. Providers typically retain records about such communications, including records of e-mails and other contacts between the user and the provider’s support services, as well records of any actions taken by the provider or user as a result of the communications.

35. As explained herein, information stored in connection with a TikTok account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a TikTok user’s IP log, stored electronic communications, and other data retained by TikTok, can indicate who has used or controlled the TikTok account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, profile contact information, message logs, photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the TikTok account at a relevant time. Further, TikTok account activity can show how and when the account was accessed or used. For example, as described herein, TikTok logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By

determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of TikTok access, use, and events relating to the crime under investigation. Additionally, location information retained by TikTok may tend to either inculcate or exculpate the TikTok account owner. Last, TikTok account activity may provide relevant insight into the TikTok account owner's state of mind as it relates to the offense under investigation. For example, information on the TikTok account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

36. Therefore, the servers of TikTok are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of TikTok, such as account access information, transaction information, and other account information.

BACKGROUND CONCERNING INSTAGRAM⁴

37. Instagram is a service owned by Meta, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510.

Specifically, Instagram is a free-access social networking service, accessible through its website

⁴ The information in this section is based on information published by Meta on its public websites, including, but not limited to, the following webpages: "Obtaining information about someone's Instagram account" (<https://help.instagram.com/232762833582105>) and "Information for law enforcement authorities" (<https://about.meta.com/actions/safety/audiences/law/guidelines>).

and its mobile application, that allows subscribers to acquire and use Instagram accounts, like the target account(s) listed in Attachment A, through which users can share messages, multimedia, and other information with other Instagram users and the general public.

38. Meta collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Meta keeps records of changes made to this information.

39. Meta also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

40. Each Instagram account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Instagram users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

41. Instagram users can also connect their Instagram and Facebook accounts to utilize certain cross-platform features, and multiple Instagram accounts can be connected to a single Facebook account. Instagram accounts can also be connected to certain third-party websites and mobile apps for similar functionality. For example, an Instagram user can "tweet" an image

uploaded to Instagram to a connected Twitter account or post it to a connected Facebook account or transfer an image from Instagram to a connected image printing service. Meta maintains records of changed Instagram usernames, associated Instagram accounts, and previous and current connections with accounts on Meta and third-party websites and mobile apps.

42. Instagram users can “follow” other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also “block” other users from viewing their posts and searching for their account, “mute” users to avoid seeing their posts, and “restrict” users to hide certain activity and prescreen their comments. Instagram also allows users to create a “close friends list” for targeting certain communications and activities to a subset of followers.

43. Users have several ways to search for friends and associates to follow on Instagram, such as by allowing Meta to access the contact lists on their devices to identify which contacts are Instagram users. Meta retains this contact data unless deleted by the user and periodically syncs with the user’s devices to capture changes and additions. Users can similarly allow Meta to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

44. Each Instagram user has a profile page where certain content they create and share (“posts”) can be viewed either by the general public or only the user’s followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography (“Bio”), and a website address.

45. One of Instagram's primary features is the ability to create, edit, share, and interact with photos and short videos. Users can upload photos or videos taken with or stored on their devices, to which they can apply filters and other visual effects, add a caption, enter the usernames of other users ("tag"), or add a location. These appear as posts on the user's profile. Users can remove posts from their profiles by deleting or archiving them. Archived posts can be reposted because, unlike deleted posts, they remain on Meta's servers.

46. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Instagram. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). An Instagram post created by one user may appear on the profiles or feeds of other users depending on a number of factors, including privacy settings and which users were tagged or mentioned.

47. An Instagram "story" is similar to a post but can be viewed by other users for only 24 hours. Stories are automatically saved to the creator's "Stories Archive" and remain on Meta's servers unless manually deleted. The usernames of those who viewed a story are visible to the story's creator until 48 hours after the story was posted.

48. Instagram allows users to broadcast live video from their profiles. Viewers can like and add comments to the video while it is live, but the video and any user interactions are removed from Instagram upon completion unless the creator chooses to send the video to IGTV, Instagram's long-form video app.

49. Instagram Direct, Instagram's messaging service, allows users to send private messages to select individuals or groups. These messages may include text, photos, videos,

posts, videos, profiles, and other information. Participants to a group conversation can name the group and send invitations to others to join. Instagram users can send individual or group messages with “disappearing” photos or videos that can only be viewed by recipients once or twice, depending on settings. Senders can’t view their disappearing messages after they are sent but do have access to each message’s status, which indicates whether it was delivered, opened, or replayed, and if the recipient took a screenshot. Instagram Direct also enables users to video chat with each other directly or in groups.

50. Instagram offers services such as Instagram Checkout and Facebook Pay for users to make purchases, donate money, and conduct other financial transactions within the Instagram platform as well as on Facebook and other associated websites and apps. Instagram collects and retains payment information, billing records, and transactional and other information when these services are utilized.

51. Instagram has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be “followed” to generate related updates from Instagram. Meta retains records of a user’s search history and followed hashtags.

52. Meta collects and retains location information relating to the use of an Instagram account, including user-entered location tags and location information used by Meta to personalize and target advertisements.

53. Meta uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads,

offers, and other sponsored content. Meta maintains related records for Instagram users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

54. In some cases, Instagram users may communicate directly with Meta about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Meta typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

55. For each Instagram user, Meta collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

56. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

57. For example, the stored communications and files connected to an Instagram account may provide direct evidence of the offenses under investigation. Based on my training

and experience, instant messages, photos, and videos are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

58. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Meta can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, messaging logs, photos, and videos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

59. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

60. Therefore, Meta's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Instagram. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

61. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require TikTok and Meta to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachments B-1 and B-2, respectively. Upon receipt of the information described in Section I of Attachments B-1 and B-2, government-authorized persons will review that information to locate the items described in Section II of Attachments B-1 and B-2.

CONCLUSION

62. Based on the foregoing, I request that the Court issue the proposed search warrant.

63. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute these warrants by serving them on TikTok and Meta. Because the warrants will be served on TikTok and Meta, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Sworn to under the pains and penalties of perjury,

Craig A. Graham
Special Agent



Craig A. Graham
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____ <i>(specify reliable electronic means)</i>	
_____ <i>Date</i>	_____ <i>Judge's signature</i>
_____ <i>City and State</i>	_____ <i>Printed name and title</i>

ATTACHMENT A-1

Property to be Searched

This warrant applies to information associated with the TikTok username @tacobell99948 and TikTok username @juvajanga (the “TIKTOK ACCOUNTS”) and from November 1, 2023 to present, that is stored at premises owned, maintained, controlled, or operated by TikTok, Inc. (“TikTok”), a company which is headquartered at 5800 Bristol Parkway, Suite 100, Culver City, California.

ATTACHMENT A-2

Property to be Searched

This warrant applies to information associated with Instagram account kwaxle and Instagram account 2fine4youbbyyy (the “INSTAGRAM ACCOUNTS”) and from November 1, 2023 to present, that is stored at premises owned, maintained, controlled, or operated by Meta Platforms, Inc. a company headquartered at 1 Meta Way, Menlo Park, California.

ATTACHMENT B-1

Particular Things to be Seized

I. Information to be disclosed by TikTok, Inc. (“TikTok”)

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of TikTok, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to TikTok, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), TikTok is required to disclose the following information to the government for each user ID listed in Attachment A-1:

- (a) All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- (b) All activity logs for the account and all other documents showing the user’s posts and other TikTok activities from account creation to present;
- (c) All photos and videos uploaded by that user ID, including Exchangeable Image File (“EXIF”) data and any other metadata associated with those photos and videos;
- (d) All profile information; status updates; videos, photographs, articles, and other items; notes; Memories; friend/contact lists, including the contacts’ TikTok user identification numbers; groups and networks of which the user is a member, including the groups’ identification numbers; future and past event postings;

rejected “friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of TikTok applications;

- (e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, advertising ID, and user agent string;
- (f) All other records and contents of communications and messages made or received by the user from creation to present, including all Messenger activity, private messages, chat history, video and voice calling history, and pending “friend” requests;
- (g) All location information;
- (h) All IP logs, including all records of the IP addresses that logged into the account;
- (i) All records of the account’s usage of TikTok features;
- (j) All past and present lists of friends/contacts created by the account;
- (k) All records of TikTok searches performed by the account from creation to present;
- (l) The types of service utilized by the user;
- (m) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

- (n) All privacy settings and other account settings, including privacy settings for individual messages and activities, and all records showing which TikTok users have been blocked by the account;
- (o) Records of any TikTok accounts that are linked to the account by machine cookies (meaning all TikTok user IDs that logged into TikTok by the same machine as the account); and
- (p) All records pertaining to communications between TikTok and any person regarding the user or the user's TikTok account, including contacts with support services and records of actions taken.

TikTok is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2422(b) and 2252(a)(2), including, for the TIKTOK ACCOUNTS listed in Attachment A-1, information pertaining to the following matters:

- (a) Communications of a sexual nature involving minors on TikTok; messaging, in any format, that involves the transfer of obscene material; and communications, in any format, designed to persuade, entice, induce, or coerce a minor into engaging in sexual activity.

- (b) Evidence indicating how and when the TikTok account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;
- (c) Evidence indicating the TikTok account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT B-2

Particular Things to be Seized

I. Information to be disclosed by Meta Platforms, Inc. (“Meta”)

To the extent that the information described in Attachment A is within the possession, custody, or control of Meta, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or other information that has been deleted but is still available to Meta, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Meta is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- A. All business records and subscriber information, in any form kept, pertaining to the account, including:
 - 1. Identity and contact information (past and current), including full name, e-mail addresses, physical address, date of birth, phone numbers, gender, hometown, occupation, websites, and other personal identifiers;
 - 2. All Instagram usernames (past and current) and the date and time each username was active, all associated Instagram and Facebook accounts (including those linked by machine cookie), and all records or other information about connections with Facebook, third-party websites, and mobile apps (whether active, expired, or removed);

3. Length of service (including start date), types of services utilized, purchases, and means and sources of payment (including any credit card or bank account number) and billing records;
 4. Devices used to login to or access the account, including all device identifiers, attributes, user agent strings, and information about networks and connections, cookies, operating systems, and apps and web browsers;
 5. All advertising information, including advertising IDs, ad activity, and ad topic preferences;
 6. Internet Protocol (“IP”) addresses used to create, login, and use the account, including associated dates, times, and port numbers, from November 1, 2023 to Present;
 7. Privacy and account settings, including change history; and
 8. Communications between Meta and any person regarding the account, including contacts with support services and records of actions taken;
- B. All content (whether created, uploaded, or shared by or with the account), records, and other information relating to videos (including live videos and videos on IGTV), images, stories and archived stories, past and current bios and profiles, posts and archived posts, captions, tags, nametags, comments, mentions, likes, follows, followed hashtags, shares, invitations, and all associated logs and metadata, from November 1, 2023 to Present;

C. All content, records, and other information relating to communications sent from or received by the account November 1, 2023 to Present, including but not limited to:

1. The content of all communications sent from or received by the account, including direct and group messages, and all associated multimedia and metadata, including deleted and draft content if available;
2. All records and other information about direct, group, and disappearing messages sent from or received by the account, including dates and times, methods, sources and destinations (including usernames and account numbers), and status (such as delivered, opened, replayed, screenshot);
3. All records and other information about group conversations and video chats, including dates and times, durations, invitations, and participants (including usernames, account numbers, and date and time of entry and exit); and
4. All associated logs and metadata;

D. All content, records, and other information relating to all other interactions between the account and other Instagram users November 1, 2023 to Present, including but not limited to:

1. Interactions by other Instagram users with the account or its content, including posts, comments, likes, tags, follows (including unfollows,

approved and denied follow requests, and blocks and unblocks), shares, invitations, and mentions;

2. All users the account has followed (including the close friends list), unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow, and of users who have followed, unfollowed, blocked, unblocked, muted, restricted, or denied a request to follow the account;

3. All contacts and related sync information; and

4. All associated logs and metadata;

E. All records of searches performed by the account November 1, 2023 to Present; and

F. All location information, including location history, login activity, information geotags, and related metadata November 1, 2023 to Present.

Meta is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2422(b) and 2252(a)(2), including, for the INSTAGRAM ACCOUNTS listed in Attachment A-2, information pertaining to the following matters:

- (a) Communications of a sexual nature involving minors on Instagram; messaging, in any format, that involves the transfer of obscene material; and communications, in any format, designed to persuade, entice, induce, or coerce a minor into engaging in sexual activity.
- (b) Evidence indicating how and when the Instagram account was accessed or used, to determine the chronological and geographic context of account access, use, and events relating to the crime under investigation and to the account owner;
- (c) Evidence indicating the Instagram account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.